CURRICULUM VITAE

ZUOBIN XIONG

25 Park Place, Suite 725, Atlanta, GA, USA, 30303
Homepage: https://zuobinxiong.github.io
Phone: (404) 862-7004, Email: zxiong2@gsu.edu

EDUCATION

- **Ph.D. Candidate** Ph.D. degree expected in June 2023
  Department of Computer Science, Georgia State University
- **M.S.**, Computer Science 2019
  Department of Computer Science, Harbin Engineering University
- **B.S.**, Mathematics 2016
  Department of Mathematics, Northeast Forestry University

RESEARCH INTERESTS

- Cyber Security
- Machine Learning
- Data Privacy
- Internet of Things

AWARDS/GRANTS

- **Student Travel Scholarship** 2023
  AAAI-2023 student travel scholarship award, supported by Association for the Advancement of Artificial Intelligence, Feb. 2023
- **Best Paper Award** 2022
  "A Self-Supervised Purification Mechanism for Adversarial Samples", by Bingyi Xie, Honghui Xu, Zuobin Xiong, Yingshu Li, and Zhipeng Cai, IEEE International Conference on Smart Data, Espoo, Finland, Aug. 2022
- **Writing Proposal** 2021
  EDU: Collaborative: Advancing Cybersecurity Learning Through Inquiry-based Laboratories on a Container-based Virtualization Platform, SaTC of NSF
- **Outstanding Graduate Research Award** 2021
  The sole one, awarded by the Department of Computer Science, Georgia State University, May 2021

TEACHING EXPERIENCE

Independent Instructor

- CSC 4520/6520 Design and Analysis of Algorithms, Fall 2019, GSU
  Undergraduate Evaluation **(4.5/5.0)**, Graduate Evaluation **(4.9/5.0)**
- CSC 4222/6222 Cyber Security, Spring 2021, GSU
  Undergraduate Evaluation **(4.5/5.0)**, Graduate Evaluation **(4.5/5.0)**

Teaching Assistant

- CSC 4740/6740 Data Mining, Spring 2019, Spring 2020, GSU
- CSC 4222/6222 Cyber Security, Fall 2020, GSU
- CSC 4520/6520 Design and Analysis of Algorithms, Fall 2021, GSU
- CSC 8920 Private and Secure AI, Spring 2022, GSU

PUBLICATIONS

Submissions Under-Review

1. **Zuobin Xiong**, Wei Li, and Zhipeng Cai, "Exact-Fun: An Exact and Efficient Federated Unlearning Approach", submitted to ACM SIGMOD/PODS 2023
2. **Zuobin Xiong**, Wei Li, and Zhipeng Cai, "FUNREAD: Towards Machine Unlearning in Federated Setting", submitted to IEEE Internet of Things Journal
3. Linyu Jiang, Yukun Yan, Zhihong Tian, **Zuobin Xiong** and Qilong Han, "Personalized Sampling Graph Collection with Local Differential Privacy for Link Prediction", submitted to World Wide Web Journal

Peer-Reviewed Journals

4. **Zuobin Xiong**, Zhipeng Cai, Chunqiang Hu, Daniel Takabi, and Wei Li, "Towards Neural Network-based Communication System: Attack and Defense", IEEE Transactions on Dependable and Secure Computing (TDSC), Early Access. (IF: 6.791)
5. Zhipeng Cai, **Zuobin Xiong**, Honghui Xu, Peng Wang, Wei Li, and Yi Pan, "Generative Adversarial Networks: A Survey Toward Private and Secure Applications", ACM Computing Surveys (CSUR), Vol. 54, No. 6, Jul. 2022. (IF: 14.324)
6. Jinbao Wang, **Zuobin Xiong**, Qilong Han, Xixian Han, and Donghua Yang, "Top-k Socially Constrained Spatial Keyword Search in Large SIoT Networks", IEEE Internet of Things Journal (IoT-J), Vol. 9, No. 12, Jun. 2022. (IF: 10.238)
7. **Zuobin Xiong**, Zhipeng Cai, Daniel Takabi, and Wei Li, "Privacy Threat and Defense for Federated Learning with Non-iid Data in AIoT", IEEE Transactions on Industrial Informatics (TII), Vol. 18, No. 2, Feb. 2022. (IF: 11.648)

8. Xiaoling Tao, Yang Peng, Feng Zhao, Changsong Yang, Baohua Qiang, Yufeng Wang, and **Zuobin Xiong**, "Gated Recurrent Unit-based Parallel Network Traffic Anomaly Detection using Subagging Ensembles", Ad Hoc Networks, Vol. 116, 2021. (IF: 4.816)

9. **Zuobin Xiong**, Zhipeng Cai, Qilong Han, Arwa Alrawais, and Wei Li, "ADGAN: Protect Your Location Privacy in Camera Data of Auto-Driving Vehicles", IEEE Transactions on Industrial Informatics (TII), Vol. 17, No. 9, Sept. 2021. (IF: 11.648)

10. Gesu Li, Guisheng Yin, **Zuobin Xiong**, and Fukun Chen, "CGPP-POI: A Recommendation Model Based on Privacy Protection", Wireless Communications and Mobile Computing, Vol. 2021, Aug. 2021.

11. **Zuobin Xiong**, Honghui Xu, Wei Li, and Zhipeng Cai, "Multi-Source Adversarial Sample Attack on Autonomous Vehicles", IEEE Transactions on Vehicular Technology (TVT), Vol. 70, No. 3, Mar. 2021. (IF: 6.239)

12. Qilong Han, **Zuobin Xiong**, and Kejia Zhang, "Research on Trajectory Data Releasing Method via Differential Privacy Based on Spatial Partition", Security and Communication Networks, Vol. 2018, Nov. 2018.

Peer-Reviewed Conference Publications

13. **Zuobin Xiong**, Wei Li, and Zhipeng Cai, "Federated Generative Model on Multi-Source Heterogeneous Data in IoT", accepted by AAAI Conference on Artificial Intelligence (AAAI), Washington, DC, USA, Feb. 2023. **(Acceptance Ratio: 19.6%)**

14. Guangxi Lu, **Zuobin Xiong**, Jing Meng, and Wei Li, "Pairwise Gaussian Graph Convolutional Networks: Defense Against Graph Adversarial Attack", accepted by IEEE Global Communications Conference (GLOBECOM), Rio de Janeiro, Brazil, Dec. 2022.

15. Guangxi Lu, **Zuobin Xiong**, and Wei Li, "Decentralized Federated Learning: A Defense against Gradient Inversion Attack", accepted by EAI WiCON, Dallas, USA, Nov. 2022.

16. Bingyi Xie, Honghui Xu, **Zuobin Xiong**, Yingshu Li, and Zhipeng Cai, "A Self-Supervised Purification Mechanism for Adversarial Samples", IEEE International Conference on Smart Data, Espoo, Finland, Aug. 2022. (**Best Paper Award**)

17. Lijie Li, Shuangyang Hu, Junhao Chen, Ye Wang, and **Zuobin Xiong**, "Exp-SoftLexicon Lattice Model Integrating Radical-Level Features for Chinese NER", International Conference on Software Engineering & Knowledge Engineering, Pittsburgh, USA, Jul. 2022.

18. **Zuobin Xiong**, Wei Li, Qilong Han, and Zhipeng Cai, "Privacy-Preserving Auto-Driving: a GAN-based Approach to Protect Vehicular Camera Data", IEEE International Conference on Data Mining (ICDM), Beijing, China, Nov. 2019. **(Acceptance Ratio: 9.08%)**

INVITED TALKS

- Invited Speaker.
  "Privacy Threats and Defense in Federated Learning". University of Electronic Science and Technology of China, Department of Computer Science, Aug. 2022, Virtual.
- Invited Speaker.
  "Towards Privacy Preservation of Federated Learning in Artificial Intelligence of Things". Virginia Commonwealth University, Department of Electrical and Computer Engineering, Sept. 2022, Virtual.
- Invited Speaker.
  "On the Privacy Inference and Protection of Federated Learning". Harbin Engineering University, College of Computer Science and Technology, Nov. 2022, Virtual.

PROFESSIONAL ACTIVITIES

- Student Member of IEEE
- Student Member of IEEE branch at GSU, 2019-now
- Reviewer for Discrete Mathematics, Algorithms and Applications (DMAA),
- Reviewer for IEEE Transactions on Industrial Informatics (TII)
- Reviewer for IEEE Transactions on Vehicular Technology (TVT)
- Reviewer for IEEE Internet of Things Journal (IoT-J)
- Reviewer for IEEE Transactions on Wireless Communications (TWC)
- Reviewer for IEEE Transactions on Knowledge and Data Engineering (TKDE)
- Reviewer for IEEE Transactions on Computational Social Systems (TCSS)
- Reviewer for IEEE Global Communications Conference (Globecom)
- Reviewer for IEEE Cyber Science and Technology Congress
- Reviewer for Elsevier Neurocomputing
- Reviewer for Elsevier Computer & Security
- Reviewer for Elsevier Computer Communications
- Reviewer for Security and Communication Networks
- Reviewer for Scientific Reports - Nature